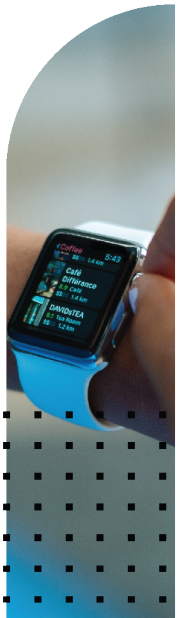
Release Notes

FortiOS 7.0.13



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 26, 2023
FortiOS 7.0.13 Release Notes
01-7013-950993-20231026

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-10-26	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.0.13 build 0566.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.13 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-400F, FG-401F, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 7.0.13. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0566.

FG-80F-DSL	is released on build 6913.
FG-900G	is released on build 6902.

FG-901G	is released on build 6902.
FG-1000F	is released on build 6903.
FG-1001F	is released on build 6903.
FG-3200F	is released on build 6912.
FG-3201F	is released on build 6912.
FG-3700F	is released on build 6912.
FG-3701F	is released on build 6912.
FG-4800F	is released on build 6912.
FG-4801F	is released on build 6912.
FWF-80F-2R-3G4G-DSL	is released on build 6913.
FWF-81F-2R-3G4G-DSL	is released on build 6913.

Special notices

Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1 and later:

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1 and later.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms running FortiOS 7.0.1 and later, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

IP pools and VIPs are now considered local addresses

In FortiOS 7.0.13 and later, all IP addresses used as IP pools and VIPs are now considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is considered a destination for those IP addresses and can receive reply traffic at the application layer.

Previously in FortiOS 7.0.1 to 7.0.12, this was not the case. For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
    edit <id>
        set fec enable
    next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.0.13 features.

SMB drive mapping with ZTNA access proxy

In FortiOS 7.0.12 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

One way to solve the issue is to enter the credentials into Windows Credential Manager in the form of `domain\username`.

Another way to solve the issue is to leverage the KDC proxy to issue a TGT (Kerberos) ticket for the remote user. See ZTNA access proxy with KDC to access shared drives for more information. This way, there is no reply in Credential Manager anymore, and the user is authenticated against the DC.

Changes in table size

Bug ID	Description
858877	Increase the number of supported dynamic FSSO IP addresses from 100 to 3000 per dynamic FSSO group. The dynamic FSSO type addresses can be pointed to FortiManager's Universal Connector, which imports the addresses from Cisco ACI or Guardicore Centra.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description
875306	Add new command to compute the SHA256 file hashes for each file in a directory. `# diagnose sys filesystem hash`

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.0.13 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.10
FortiManager	• 7.0.10
FortiExtender	• 7.0.3 and later. For compatibility with latest features, use latest 7.4 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 16
FortiClient* EMS	• 7.0.0 build 0042 or later
FortiClient* Microsoft Windows	• 7.0.0 build 0029 or later
FortiClient* Mac OS X	• 7.0.0 build 0022 or later
FortiClient* Linux	• 7.0.0 build 0018 or later
FortiClient* iOS	• 6.4.6 build 0507 or later
FortiClient* Android	• 6.4.6 build 0539 or later
FortiSandbox	• 2.3.3 and later

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.0.0, use FortiClient 7.0.0.

Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice
17. FortiDeceptor
18. FortiAI/FortiNDR
19. FortiTester
20. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.13. When Security Fabric is enabled in FortiOS 7.0.13, all FortiGate devices must be running FortiOS 7.0.13.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings

- admin user account
- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 and later need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

In the case when customers are using the following settings in 6.4:

```
config system settings
    set default-voip-alg-mode proxy-based
end
```

```
config firewall policy
    edit 0
        set inspection-mode flow
        unset voip-profile
    next
end
```

In 6.4, by default, SIP traffic is handled by proxy-based SIP ALG even though no VoIP profile is specified in a firewall policy.

After upgrading, the firewall policy will remain in `inspection-mode flow` but handled is by flow-based SIP inspection.

Due to the difference in which the SIP traffic is handled by flow-based SIP versus proxy-based SIP ALG inspection in 7.0.0 and later, if customers want to maintain the same behavior after upgrading, they can manually change the firewall policy's `inspection-mode` to `proxy`:

```
config firewall policy
    edit 0
        set inspection-mode proxy
        unset voip-profile
    next
end
```

Or prior to upgrading, they can assign a `voip-profile` to the firewall policies that are processing SIP traffic to force the conversion to `inspection-mode proxy` after upgrading.

L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later

If the setting is not manually updated after upgrading, the VPN connection will be established, but it will not be accessible from the internal network (office network). This setting change is necessary regardless of whether route-based or policy-based IPsec is used.

To make L2TP over IPsec work after upgrading:

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
    set eip 210.0.0.254
    set sip 210.0.0.1
    set status enable
    set usrgrp "L2tpusergroup"
end
```

   Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "l2t.root"
    next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`

- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects* > *NAT46 Policy*
- *Policy & Objects* > *NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects* > *Virtual IPs* related pages

During the upgrade process after the FortiGate reboots, the following message is displayed:

```
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log read'
```

The following output is displayed after running the diagnose command:

```
# diagnose debug config-error-log read
>>> "config" "firewall" "policy64" @ root:command parse error (error -
61)
>>> "config" "firewall" "policy46" @ root:command parse error (error -
61)
```

Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.
- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip`/`vip6` and `ippool`/`ippool6`.

Example configurations

`vip46` object:

Old configuration	New configuration

`config firewall vip46`
`edit "test-vip46-1"`
`set extip 10.1.100.155`
`set mappedip 2000:172:16:200::55`
`next`
	`config firewall vip`
	`edit "test-vip46-1"`
	`set extip 10.1.100.150`
	`set nat44 disable`
	`set nat46 enable`

Old configuration	New configuration
end	set extintf "port24" **set ipv6-mappedip 2000:172:16:200::55** next end

`ippool6` object:

Old configuration	New configuration
config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end	config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 **set nat46 enable** next end

NAT46 policy:

Old configuration	New configuration
config firewall policy46 edit 1 set srcintf "port24" set dstintf "port17" set srcaddr "all" set dstaddr "test-vip46-1" set action accept set schedule "always" set service "ALL" set logtraffic enable set ippool enable set poolname "test-ippool6-1" next end	config firewall policy edit 2 set srcintf "port24" set dstintf "port17" set action accept **set nat46 enable** set srcaddr "all" set dstaddr "test-vip46-1" set srcaddr6 "all" set dstaddr6 "all" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname6 "test-ippool6-1" next end

`vip64` object

Old configuration	New configuration
config firewall vip64 edit "test-vip64-1" set extip 2000:10:1:100::155 set mappedip 172.16.200.155 next	config firewall vip6 edit "test-vip64-1" set extip 2000:10:1:100::155 set nat66 disable **set nat64 enable**

Old configuration	New configuration
end	**set ipv4-mappedip 172.16.200.155** next end

`ippool` object

Old configuration	New configuration
config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 next end	config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 **set nat64 enable** next end

NAT64 policy:

Old configuration	New configuration
config firewall policy64 edit 1 set srcintf "wan2" set dstintf "wan1" set srcaddr "all" set dstaddr "test-vip64-1" set action accept set schedule "always" set service "ALL" set ippool enable set poolname "test-ippool4-1" next end	config firewall policy edit 1 set srcintf "port24" set dstintf "port17" set action accept **set nat64 enable** set srcaddr "all" set dstaddr "all" set srcaddr6 "all" set dstaddr6 "test-vip64-1" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname "test-ippool4-1" next end

ZTNA configurations and firewall policies

Since FortiOS 7.0.2, ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration.

When upgrading from FortiOS 7.0.1 or below:

- If an `access-proxy` type `proxy-policy` does not have a `srcintf`, then after upgrading it will be set to `any`.
- To display the `srcintf` as *any* in the GUI, *System* > *Feature Visibility* should have *Multiple Interface Policies* enabled.
- All full ZTNA firewall policies will be automatically removed.

Default DNS server update

Starting in FortiOS 7.0.4, if both primary and secondary DNS servers are set to use the default FortiGuard servers prior to upgrading, the FortiGate will update them to the new servers and enable DoT after upgrading. If one or both DNS servers are not using the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

Product integration and support

The following table lists FortiOS 7.0.13 product integration and support information:

Web browsers	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 0312 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2022 Standard
	  • Windows Server 2022 Datacenter
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

AV Engine	• 6.00294
IPS Engine	• 7.00176

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESX	• Versions 4.0 and 4.1
VMware ESXi	• Versions 6.5, 6.7, and 7.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 113 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Ventura 13	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 7.0.13. To inquire about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
877613	*Mark as Reject* can be still chosen as an *Action* in an *Anti-Spam Block/Allow List* in the GUI.

Anti Virus

Bug ID	Description
911332	When UTM status is enabled and the AV profile has no configuration, all SLL traffic is dropped and there is no WAD output.
923883	The FortiGate may display an error log in the crash log due to AV delta update. In case of failure, a full successful AV update is done.

Application Control

Bug ID	Description
939565	`can not query meta rules list` seen on graceful/non-graceful upgrade.

DNS Filter

Bug ID	Description
931998	DNS filter flow external domain AAAA query can still check the default category but not the remote category.

Endpoint Control

Bug ID	Description
897048	FortiOS should support EMS 7.2.1 auth API status code changes.
913324	GUI repeated calls to the EMS API, which can cause EMS to not authorize the FortiGate correctly.

Explicit Proxy

Bug ID	Description
817582	When there are many users authenticated by an explicit proxy policy, the *Firewall Users* widget can take a long time to load. This issue does not impact explicit proxy functionality.
859693	Sessions between the explicit proxy and server stay in SYN_SENT state when using IP pools in the explicit proxy policy for source NAT, even though the sessions have established. Traffic is not impacted.
863665	Denied explicit proxy keeps using the Fortinet_CA_SSL default certificate, even if the configured certificate is different.
889300	Wrong source IP address used for packets through explicit proxy routed to a member of SD-WAN interface.
923302	Cannot send picture through web explicit proxy.

Firewall

Bug ID	Description
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic.
752267	*Load Balance Monitor* detects a server in standby mode as being down.
848058	NPD failed to parse zone in the source interface of a DoS/ACL policy and failed to offload.
851212	After traffic flow changes to FGSP peer from owner, iprope information for synchronized sessions does not update on the peer side.
861981	Traffic drops between two back-to-back EMAC VLAN interfaces.
879225	Egress interface cannot be intermittently matched for Wake-on-LAN (broadcast) packets.

Bug ID	Description
879705	Traffic issues occur with virtual servers after upgrading.
884908	Implicit deny policy is allowing "`icmp/0/0`" traffic.
895946	Access to some websites fails after upgrading to FortiOS 7.2.3 when the firewall policy is in flow-based inspection mode.
897849	*Firewall Policy* list may show empty sequence grouping sections if multiple policies are sharing the same `global-label`.
912089	Optimize CPU usage caused by a rare error condition which leads to no data being sent to the collector.
914939	UDP fragments dropped due to DF being set. Only the `set honor-df global` option.
926029	New sessions are created and evaluated after a certain number of UDP packets, even if `set block-session-timer 300` is set.
951373	Traffic shaping is not matching the correct queue for outbound traffic.

FortiView

Bug ID	Description
894957	On *FortiView Websites*, the real time view is always empty if disk logging is disabled.

GUI

Bug ID	Description
863126	In an environment where the Security Fabric is enabled and there are more than 100 firewall object conflicts between the root and downstream FortiGates, the *Firewall Object Synchronization* pane does not list the details.
892207	Unable to authorize a newly discovered FortiAP from the *WiFi Controller* > *Managed FortiAPs* page.
893560	When private data encryption is enabled, the GUI may become unresponsive and HA may fail to synchronize the configuration.
907041	*Network* > *SD-WAN* > *SD-WAN Zones* and *SD-WAN Rules* pages do not load if a shortcut tunnel is triggered.
916236	GUI policy table cannot display sequence grouping section titles correctly if they are duplicated in the global label.
919390	Disabling `gui-wireless-controller` on the root VDOM impacts other VDOMs (unable to add or show WiFi widgets on first load).

Bug ID	Description
943949	When editing an interface description in GUI, the following characters are not allowed: <, >, (,), #, ', and ".
946878	FortiGate HA management interface in the GUI not allowing multiple route entries, but the CLI does allow them.

HA

Bug ID	Description
703614	HA secondary synchronization fails and keeps rebooting when the primary has a split port configuration.
771316	Platforms in an HA environment get stuck in a reboot loop while attempting to synchronize configurations that differ in split ports.
805663	After upgrading, rebooting the primary in HA (A-A) results in unusually high bandwidth utilization on redundant interfaces.
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.
838571	After an HA split-brain event, the PPPoE interfaces are not recovered.
870312	On a FortiGate HA cluster, both primary and secondary units are displayed as the *Primary* on the GUI top banner, and as `Current HA mode` in the CLI.
875984	FortiGate is going to out-of-sync after changing parameters of VDOM link interfaces.
881337	Adding a VLAN interface on any VDOM causes BGP flapping and VIP connectivity issues on VDOMs in vcluster2.
893041	Cannot access out-of-band IPv6 address on HA secondary unit.
897865	When NP7 platforms enable the GTP enhanced mode it does not use uninterruptible upgrade.
902945	Lost management connectivity to the standby node via in-band management.
904318	FortiGate sent ARP request with loopback IP address as the source address.
912665	FGCP primary-secondary cluster only uses one `session-sync-dev`, in spite of having multiple `session-sync-dev`.
916216	When adding a new interface, some other interfaces have the wrong virtual MAC address.
920233	The *System* > *HA* page is missing from the GUI on 5K models.
931724	HA events not synchronizing between members, leading to unexpected HA status.
950868	Traffic is not forwarded on L2 peer to keep FGSP with an available L2 connection.
953167	Access to console and SSH is lost due to a specific configuration.

Hyperscale

Bug ID	Description
915796	With an enabled hyperscale license, in some cases with exception traffic (like ICMP error traverse), the FortiGate may experience unexpected disruptions when handling the exception traffic.
924196	Device is rebooting randomly when driver processes exception packets.

ICAP

Bug ID	Description
884339	When the algo process starts up, it attempts to build an ICAP profile without allocating memory beforehand.

Intrusion Prevention

Bug ID	Description
823583	Failover on clustered web application using keepalived daemon does not work seamlessly.
842523	IPv6 with hardware offloading and IPS drops traffic (`msg="anti-replay check fails, drop).`
860315	Unexpected behavior in IPS engine when executing `diagnose test application ipsmonitor 44.`
862830	`[?Q?ci_" sekret=]` causes the parser to create a new field, `"sekret=".`
873975	Source MAC changes and the packet drops due to both sides of the session using the same source MAC address.
882593	HTTPS traffic slows when IPS with NTurbo is used over a virtual wire pair.
892302	Constant reloading of the external domain table is causing high CPU due to lock contention when reloading the table.
926639	Constant reloading of the shared memory external domain table is causing high CPU usage due to lock contention when reloading the table.
952270	IPS logs for VIP traffic shows external IP as a destination for some signatures.

IPsec VPN

Bug ID	Description
766750	FortiGate does not accept secondary tunnel IP address in the same subnet as the primary tunnel.
812229	ASCII-encoded byte code of remote gateway IP is displayed in the GUI and CLI when a VPN tunnel is formed using IKEv1 or v2 if the `peer-id` is not configured.
872769	Proxy ARP stops working for a client connected to a dialup IPsec when the previous VPN was established and is deleted.
885333	Forwarded broadcast traffic on ADVPN shortcut tunnel interface dropped.
887800	In an L2TP configuration, `set enforce-ipsec enable` is not working as expected after upgrading.
920725	IPsec tunnels that have external DHCP services for IP assignment have an extra selector added after upgrading to 7.0.11.
922064	Firewall becoming unresponsive to DPD/IKE messages, causing IPsec VPNs to drop.
926048	Traffic through a shortcut got dropped after an HA failover.
928774	IPsec VPN connection should allow % in FortiClient Connect REG_PASSWD field.
932112	EAP in IKEv2 dialup IPsec connection does not work with two firewall polices, each using both the IKEv2 interface and user group.
949086	Policy route is not matching ESP traffic.
954614	IPsec phase 2 negotiation fails with `failed to create dialup instance, error 22` error message.

Log & Report

Bug ID	Description
831441	The forward traffic log show exabytes of data being sent and received from external to external IP addresses in multiple VDOMs.
860822	When viewing logs on the *Log & Report* > *System Events* page, filtering by *domain\username* does not display matching entries.
879228	FortiAnalyzer override settings are not taking effect when `ha-direct` is enabled.
893199	The FortiGate does not generate deallocate/allocate logs of the first IP pool when the first IP pool has been exhausted.
902797	IPS alert email not being sent when IPS attack event has triggered.

Bug ID	Description
908856	Traffic log can show exabytes of data sent and received when generating log task is triggered from userspace.
932537	If Security Rating is enabled to run on schedule (every 4 hours), the FortiGate can unintentionally send local-out traffic to fortianalyzer.forticloud.com during the Security Rating run.

Proxy

Bug ID	Description
783549, 902613, 921247	An error condition occurs in WAD caused by multiple outstanding requests sent from client to server with UTM enabled.
785927	Unexpected behavior in WAD when multiple DHCP servers are configured.
820096	CPU usage issue in proxyd caused by the absence of TCP teardown.
863132	Proxy mode inspection is slow when testing a single TCP stream from fast.com, which causes bandwidth slowness on FG-100F and FG-200F devices.
882182	Unexpected behavior in WAD due to the activation of firewall protocol options, with both client and server comfort features enabled.
897347	Memory usage issue caused by the WAD user info process while authenticating the LDAP users.
912116	Website (li***.cz) is not working in proxy inspection mode with deep inspection and web filter applied.

REST API

Bug ID	Description
892237	Updating the HA monitor interface using the REST API PUT request fails and returns a -37 error.
903908	The forticron application crashes when restoring a VDOM configuration.
948356	An error condition occurs in HTTPSD when a REST API request is sent with invalid parameters.

Routing

Bug ID	Description
775752	`link-down-failover` does not bring the BGP peering down.
779330	The SD-WAN service with `load-balance` mode is disabled, even though there is still a member alive in the service rule.
827565	Using `set load-balance-mode weight-based` in SD-WAN implicit rule does not take effect occasionally.
839669	Static route through an IPsec interface is not removed after the BFD neighbor goes down.
858248	OSPF summary address for route redistribution from static route via IPsec VPN always persists.
875668	SD-WAN SLA log information has incorrect inbound and outbound bandwidth values.
900941	`config redistribute` routing subsections cannot be configured when in workspace mode.
906896	Make OSPFv3 update the translator role and translated Type-5 LSA when the ASBR table is updated.
922491	Static routes are installed on hub FortiGate with `add-route` disabled in ADVPN scenario.
924940	When there are a lot of policies (several thousands), the interface member selection for the *SD-WAN Zone* dialog may take up to a minute to load.
928152	FortiGate generates two OSPF stub entries for the same prefix after upgrading from 6.4 to 7.0.

Security Fabric

Bug ID	Description
851656	Sessions with `csf_syncd_log` flag in a Security Fabric are not logged.
912592	Allow comments and IP addresses to be on the same line for external IP address threat feeds.
912917	Send Fabric API calls with pagination filter.
917024	Unexpected behavior in Security Fabric daemon (CSFD) caused by triggering HA failover while using Security Fabric.
920391	Non-management VDOM is not allowed to set a `source-ip` for `config system external-resource`.
922896	Azure SDN connector always uses HA management port for DNS resolve. This might not work on premises where the HA management port does not have a public IP address assigned.

SSL VPN

Bug ID	Description
631809	Configuring thousands of `mac-addr-check-rule` in portal makes the CPU spike significantly if several hundreds of users are connecting to the FortiGate, thus causing SSL VPN packet drops.
843756	Customer bookmark (*.tr***.pt) is not accessible when using SSL VPN web mode.
859088	FortiGate adds extra parenthesis and causes clicking all links to fail in SSL VPN web mode.
871229	SSL VPN web mode does not load when connecting to customer's internal site.
873516	FortiGate misses the closing parenthesis when running the function to rewrite the URL.
875167	Webpage opened in SSL VPN web portal is not displayed correctly.
881220	Found bad login for SSL VPN web-based access when enabling URL obscuration.
881268	Disconnecting from SSL VPN using the *SSL-VPN* widget does not disconnect the SSL VPN tunnel.
884869	Web mode bookmark showing blank page due to JS rewrite.
885978	Some buttons in URL are not working in SSL VPN web mode.
886989	SSL VPN process reaches 99% CPU usage when HTTP back-end server resets the connection in the middle of a post request.
887345	When a user needs to enter credentials through a pop-up window, the key events for modification key detected by SDL were ignored.
887674	FortiGate will intermittently stop accepting new SSL VPN connections across all VDOMs.
897385	Internal website keeps asking for credential with SSL VPN web mode.
897665	The external DHCP server is not receiving hostnames in SSL VPN and DHCP relay.
904919	DHCP option 12 hostname needed for SSL VPN with external DHCP servers.
927475	SSL VPN tunnel down log message not generated when an IP address is disassociated before the old tunnel times out.
933985	FortiGate as SSL VPN client does not work on NP6 and NP6XLite devices.
950157	SS LVPN connected/disconnected endpoint event log can be in the wrong sequence.
952860	During a handshake when FortiClient sends a larger-than-MTU hello message, the packet is fragmented by IP layer and dropped by the FortiGate.

Switch Controller

Bug ID	Description
890912	FortiLink VLAN interface should be renamed from `default` to `_default` after upgrading to 7.0.10.

Bug ID	Description
893405	One discovery one transmit buffer was allocated and was not released on connection terminations.
894735	Unable to configure more than one NAC policy using the same EMS tag for different FortiSwitch groups.
911232	Security rating shows an incorrect warning for unregistered FortiSwitches on the *WiFi & Switch Controller > Managed FortiSwitches*.
920231	FortiGate loses QoS `ip-dscp-map` configuration after reboot.
936081	The `vlan-optimization {enable | disable}` and `vlan-all-mode all` configuration options disappear after upgrade or reboot.

System

Bug ID	Description
708964	CPU usage issue is observed caused by reloading the system when the system has `cfg-save` set to `revert`.
713951	Not all ports are coming up after an LAG bounce on 8 × 10 GB LAG with ASR9K. Affected platforms: FG-3960E and FG-3980E.
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled.
729912	DNS proxy does not transfer the DNS query for IPv6 neighbor discovery (ND) when client devices are using random MAC addresses, so one device can configure many IPv6 addresses.
822297	Polling fgfwpolid returns disabled policies.
828129	A disabled EMAC VLAN interface is replying to a ping.
832154	The cmdbsvr process may crash when there are many addresses and address groups that include each other recursively.
842159	FortiGate 200F interfaces stop passing traffic after some time.
855573	False alarm of the PSU2 occurs with only one installed.
859393	SNMP poll for fgExplicitProxyRequests returns 0.
862519	FortiGate 40F-3G4G WWAN connection unstable on Verizon Carrier.
866437	CPU usage issue caused by the new Linux kernel.
867663	The FEC configuration under the interface is not respected when port23 and port24 are members of an LACP and the connection is 100G. Affected platforms: FGT-340xE, FGT-360xE.
869044	If the original packet was forwarded with NAT, generated ICMP error is routed back to SNAT'ed address.

Bug ID	Description
873805	CPSS usage goes to 99% and causes initiation issues when traffic is flowing upon boot. Affected platforms: FG-40xF, FG-60xF, FG-300xF.
874292	`ssh-rsa` should be disabled under the SSH `server_host_key_algorithm`.
876853	No output of `execute sensor list` is displayed after rebooting.
879769	If the firewall session is in `check-new` mode, FortiOS will not flush its NPU offload entry when there is a MAC address update of its gateway.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.
884023	When a user is logged in as a VDOM administrator with restricted access and tries to upload a certificate (*System* > *Certificates*), the *Create* button on the *Create Certificate* pane is greyed out.
885823	Sensor showing temperature of 0.00 Celsius.
891165	Auto-script causes FortiGate to repeat commands.
892274	Daylight saving time is not applied for Cairo time zone.
892478	Interface release from cmdb and iprope keep updating when DHCP client renewal fails.
894202	Incorrect temperature calculation appears in sensor list on FG-8xF, FWF-8xF, FG-9xE, FG-10xE, FG-20xE, and FG-14xE.
894884	FSTR session ticket zero causes a memory leak.
903362	SNMP OID, fgFwPolLastUsed (1.3.6.1.4.1.12356.101.5.1.2.1.1.4), does not show the correct information about the last time a specific policy was used.
903397	After upgrading to 7.0.11, FortiOS cannot display QSFP+ transceiver information. Affected platforms: FG-110xE, FG-220xE, FG-330xE, FG-340xE, and FG-360xE.
904414	Port speed 1000auto could not link up with a Cisco switch.
904486	The FortiGate may display a false alarm message and subsequently initiate a reboot.
907339	dnsproxy process aborts due to stack buffer overflow being detected upon function return.
910269	Unexpected behavior caused by the Linux Out of Memory (OOM) killer when memory is very low.
910273	*Last reboot reason: power cycle* after rebooting due to a kernel panic is misleading.
910616	When a non-zero DSCP copied from ingress to egress packet for NAT64, the IP checksum is calculated incorrectly.
910651	All members are up on an FG-600F, but the LACP status is showing as down after upgrading.
910677	Transparent mode FortiGate does not reply to SYN ACK when communicating with FortiManager.
920085	CPU usage issue observed in dnsproxyd caused by unused wildcard FQDN.
922965	CPU usage issue observed in hasync daemon when session count is large.
922982	FortiGate does not respond to ARP requests for the IP address on the WAN port when the interface is configured as EMAC.

Bug ID	Description
923364	System goes into halt state with `Error: Package validation failed...` message in cases where there are no engine files in the FortiGate when the BIOS security level is set to 2.
924395	IPv6 local-in ping6 to management interface failed when newly configured.
925657	After a manual system administrator password change, the updated `password-expire` is not received by the FortiManager auto-update.
926035	On D-series FortiGates, a false alarm during system integrity check failure causes the firewall to reboot.
926817	Review the temperature sensor for the SoC4 system.
929821	An error condition occurred in httpsd and newcli when trying to generate a TAC report from the GUI and CLI, respectively.
939411	Multiple spawns of Hotplug process consuming high CPU resources.
940571	Memory usage issue caused by excessive log files.
942502	Kernel panic occurs when creating EMAC VLAN interfaces based on an aggregate interface with new kernel 4.1.9.
945871	DNAT does not work on software switch in explicit mode.

Upgrade

Bug ID	Description
920223	System hangs after upgrade with the following error at bootup: `cli 141 die in an exception in line 4495: Hrp`.
939011	All transparent VDOMs cannot synchronize because of `switch-controller.auto-config.policy`.

User & Authentication

Bug ID	Description
790884	The FortiGate will not send a MAC-based authentication RADIUS authentication request for one of the devices on the network.
794477	When a user's membership in AD or port range is changed, all of the user sessions are cleared.
850473	SSL VPN and firewall authentication SAML does not work when the application requires SHA-256.
858877	Dynamic address only has 100 IP addresses while FSSO group lists all 56K ACI endpoints.
868994	FortiGate receives FSSO user in the format of HOSTNAME$.

Bug ID	Description
883006	Adding a new group membership to an FSSO user terminates all the user's open sessions.
899852	FortiGate is sending Class(25) AVP with wrong length in RADIUS accounting when using 2FA with PUSH or external tokens.
901743	An error condition occurs during the processing of the UDP packets when device identification is activated on an interface.
943087	Guest management users no longer view the password automatically generated by the firewall.

VM

Bug ID	Description
901920	AWS external account list supports regional endpoints.
913696	In the periodic status check of the OCI VM status, too many API calls caused a lot of 429 errors.
921168	Restore operation overwrite passive configuration in AZURE A-P deployment based on SDN connector.
927323	Event log alert `Write Permission Violation` to read-only file on VMware after taking snapshot.
932085	In an Azure cluster, the NTP `source-ip6` (IPv6) is synchronized while the `source-ip` (IPv4) is not.
950899	Azure FortiGate keeps rebooting after upgrading to 7.0.11, and the device enters kernel panic.

VoIP

Bug ID	Description
887384	SIP session is dropped by ALG with `media type doesn't match` message.

Web Filter

Bug ID	Description
829704	Web filter is not logging all URLs properly.
878442	FortiGuard block page image (logo) is missing when the `Fortinet-Other` ISDB is used.

Bug ID	Description
916140	An error condition occurs in WAD caused by the mismatch between the SNI host and CNAME.
941045	Local rating chooses the wrong category if the URL path falsely matches to a longer local rating URL.

WiFi Controller

Bug ID	Description
875382	When accessing the managed FortiAP/Switch view with a large number of devices in the topology, the page takes a long time to load.
904349	Unable to create FortiAP profile in the GUI for dual-5G mode FortiAP U231F/U431F models. **Workaround**: use the CLI to update the profile to dual-5G mode.
905406	In `auth-logon` and `auth-logout` logs, Wi-Fi users with random public IP addresses are observed.
926999	EAP proxy daemon crashed with signal 11 and keeps reloading after receiving an empty username.

ZTNA

Bug ID	Description
888814	Unable to match first group attribute from SAML assertion for ZTNA rule.
889994	After client device information is updated, the session is closed even though all information from the session still matches the policy.
923804	ZTNA logs are showing the log message `Denied: failed to match a proxy-policy` when client device information matches the policy.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
875854	FortiOS 7.0.13 is no longer vulnerable to the following CVE Reference: • CVE-2023-28001
911617	FortiOS 7.0.13 is no longer vulnerable to the following CVE Reference: • CVE-2023-37935

Known issues

The following issues have been identified in version 7.0.13. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.

Explicit Proxy

Bug ID	Description
942612	Web proxy forward server does not convert HTTP version to the original version when sending them back to the client.

Firewall

Bug ID	Description

843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI.
	This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.
	Workaround: create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if `ALL` is the first firewall service in the list:
	`config firewall service custom`
	`edit "unused"`
	`set tcp-portrange 1`
	`next`
	`move "unused" before "ALL"`
	`end`

FortiView

Bug ID	Description
941521	On the *FortiView Web Sites* page, the *Category* filter does not work in the Japanese GUI.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. **Workaround**: use Chrome, Edge, or Safari as the browser.
755177	When upgrading firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
810225	An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
853352	On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries.
898902	In the *System* > *Administrators* dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the *Two-factor Authentication* toggle. This issue does not affect configuring other settings in the dialog. **Workaround**: use the CLI to configure `two-factor-authentication` under `config system admin`.

HA

Bug ID	Description
810286	FGSP local sessions exist after rebooting an HA pair with A-P mode, and the HW SSE/session count is incorrect.

Hyperscale

Bug ID	Description
795853	VDOM ID and IP addresses in the IPL table are incorrect after disabling EIF/EIM.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.
836976	Sessions being processed by hyperscale firewall policies with hardware logging may be dropped when dynamically changing the `log-processor` setting from `hardware` to `host` for the hardware log sever added to the hyperscale firewall policy. To avoid dropping sessions, change the `log-processor` setting during quiet periods.
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
839958	`service-negate` does not work as expected in a hyperscale deny policy.
842659	`srcaddr-negate` and `dstaddr-negate` are not working properly for IPv6 traffic with FTS.
843132	Access control list (ACL) policies added to a hyperscale firewall VDOM that is processing traffic may take longer than expected to become effective. During a transition period, traffic that should be blocked by the new ACL policy will be allowed.
843197	Output of `diagnose sys npu-session list/list-full` does not mention policy route information.
843266	Diagnose command should be available to show `hit_count/last_used` for policy route and NPU session on hyperscale VDOM.
843305	Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up.
844421	The `diagnose firewall ippool list` command does not show the correct output for overload type IP pools.
846520	NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover.
941784	Hardware session synchronization does not work on FG-480xF devices in hyperscale.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.

Log & Report

Bug ID	Description
850642	Logs are not seen for traffic passing through the firewall.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
794703	Security Rating report for *Rogue AP Detection* and *FortiCare Support* checks show incorrect results.
862424	On a FortiGate that has large tables (over 1000 firewall policies, address, or other tables), security rating reports may cause the FortiGate to go into conserve mode.

System

Bug ID	Description
847664	Console may display `mce: [Hardware Error]` error message after fresh image burn or reboot.

User & Authentication

Bug ID	Description
765184	RADIUS authentication failover between two servers for high availability does not work as expected.

VM

Bug ID	Description
800935	ESXi VLAN interface based on LACP does not work.

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the *Managed FortiAPs* page and *FortiAP Status* widget can take a long time to load. This issue does not impact FortiAP operation.

ZTNA

Bug ID	Description
848222	ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type. An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found.

Built-in IPS Engine

Bug ID	Description
835757	IPS Engine 6.004.133 crashes with signal 11.
864118	XFF does not always populate in the IPS logs.
872747	CPU utilization reaches 99% due to IPS process and ipsengine has a signal 11 crash.
886685	IPS engine has high memory usage.
887299	Traffic blocked by URL filter, even though one is not configured.
892302	Constant reloading of the external domain table is causing high CPU due to lock contention when reloading the table.
894004	Using the HTTP any protocol option offloads traffic, but when the HTTP port is specified as 80 8080, traffic is not offloaded.
897523	Issues occur with TCP SACK and TCP retransmissions by IPS/NTurbo when DPI is used.
902857	FortiGate does not forward TLS ServerHello to client when IPS is enabled with flow mode and deep inspection.
908682	First HTTPS attempt with infected EICAR file cannot be blocked by IPS Engine 7.166 in a flow mode AV profile.
911118	Static URL filter does not work on some firewalls for HTTPS connections on a custom port.
912577	DNS queries (A/AAAA) from Linux have timeouts and delays.
913230	DNS translation intermittently fails.
916992	DNS static filter does not work as expected if it is the only setting in the DNS profile.
923173	IPS engine causes FortiGate to enter conserve mode.
923836	Deep inspection and flow mode does not work for certain URLs.
929019	IPS Engine 07.002.314 crashes.
929110	A configuration with `sni-server-cert-check strict` is not blocking flow-based sessions if the CN of self-signed certificate is allowed in web filter profile's *URL Filter* table.
932111	IPS engine memory leak results in difference between FortiOS memory and IPS memory.
937578	IPS engine crashes after upgrading to 7.0.12.
938937	IPS and AV engines crash.
940344	Static URL filter is working intermittently.
945804	CPU and memory utilization goes high and causes a traffic freeze. IPS process crashes are observed with an ipsengine signal 11 crash.
947349	IPS crash occurs (06.004.162).
948627	Connection timeout or reset on specific websites occurs if a web filter profile is enabled.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com